WHAT IS CLAIMED IS:

1. A method for transmitting digital data in a form of packets through a transmission medium with error correction, each packet being formatted as a fixed number of data words, each data word having more than 1 bit, the method comprising the steps of:

encoding a sent data packet to form a sent encoded data packet, including:

applying an error detection scheme to the sent data packet to add a first error detection field to the packet to form a first Protected Packet;

applying an error correction scheme to the first Protected Packet to add a first error correction field to said first Protected Packet to form the Sent Encoded Packet;

transmitting the sent encoded data packet through the transmission medium, which may introduce errors into the packet during the transmission, the Sent Encoded Packet being received as a Received Encoded Packet at the output of the transmission medium, the Received Encoded Packet including a second Protected Packet and a second error correction field, the second Protected Packet including a second data packet and a second detection field; and

decoding the Received Encoded Packet to recover a copy of the sent data packet.

2. A method as described in claim 1, wherein the step of decoding comprises:

correcting errors, if any, in the Received Encoded Packet to recover a third Protected Packet, the third Protected Packet having a third data packet and a third detection field, the third Protected Packet including fields from the second Protected Packet with the errors being corrected, the third Protected Packet being a copy of the first Protected Packet within the power of the correction scheme.

3. A method as described in claim 2, wherein the step of decoding further comprises:

determining the integrity of the third Protected Packet; and

if the integrity is confirmed, recovering a recovered data packet from the third Protected Packet, the recovered data packet being a copy of the sent data packet within the power of the correction and detection schemes.

4. A method as described in claim 2, wherein the step of correcting errors comprises correcting one or more errors occurred in a single data word of the Sent Encoded Packet only.

5. A method as described in claim 3, wherein the step of decoding comprises generating a packet drop indicator signal if the power of the correction scheme is exceeded and the correction scheme cannot correct errors.

6. A method as described claim 3, wherein the step of decoding comprises generating a packet drop indicator signal if the integrity is not confirmed.

7. A method as described in claim 4, wherein the step of applying the error correction scheme to the first Protected Packet to add the first error correction field comprises applying an algebraic function to the data words in the first Protected Packet to generate the first error correction field.

8. A method as described in claim 2, wherein the step of correcting comprises the following steps:

applying an algebraic function to the data words in the second Protected Packet to generate a third error correction field;

applying a bitwise exclusive OR function the second and third correction fields to obtain an error syndrome value;

if an error occurred, identifying the data word which has the error and obtainng a bit pattern of the error from the error syndrome value; and

correcting the identified word in the second Protected Packet by using the obtained bit pattern to obtain the third Protected Packet.

9. A method as described in claim 7, wherein the step of applying the algebraic function comprises performing a N-dimensional parity calculation.

10. A method as described in claim 9, wherein the step of applying N-dimensional parity calculation comprises performing a 3D (three dimensional) parity calculation.

11. A method as described in claim 1, wherein the step of applying the error detection scheme comprises applying an algebraic function to the data words in the sent data packet to generate the first detection field.

12. A method as described in claim 11, wherein the step of applying the algebraic function comprises applying one or more of the following functions: CRC-16, CRC-32 and a checksum.

13. A method as described in claim 3, wherein the step of determining the integrity comprises:

applying said error detection scheme to the third data packet to generate a fourth detection field;

comparing the third and fourth detection fields;

confirming the integrity of the third Protected Packet, if the third and fourth detection fields are equal.

14. A method as described in claim 10, wherein the transmitting of data is performed so that each data word is an 8-bit byte, and each data packet has not more than 64 bytes.

15. A method as described in claim 1, wherein transmitting of the sent encoded data packet through the transmission medium comprises transmitting said packet through the transmission link.

16. A method as described in claim 15, wherein transmitting the sent encoded data packet through the transmission link comprises transmitting said packet through the link which provides line coding of the transmitted data.

17. A method as described in claim 16, wherein the transmitting the packet through the line coded link comprises transmitting the packet through the link, which provides 8B/10B line coding.

18. A system for transmitting digital data in a form of packets through a transmission medium with error correction, each packet being formatted as a fixed number of data words, each data word having more than 1 bit, the system comprising:

means for encoding a sent data packet to form a sent encoded data packet, including:

means for applying an error detection scheme to the sent data packet to add a first error detection field to the packet to form a first Protected Packet;

means for applying an error correction scheme to the first Protected Packet to add a first error correction field to said first Protected Packet to form the Sent Encoded Packet;

means for transmitting the sent encoded data packet through the transmission medium, which may introduce errors into the packet during the transmission, the Sent Encoded Packet being received as a Received Encoded Packet at the output of the transmission medium, the Received Encoded Packet including a second Protected Packet and a second error correction field, the second Protected Packet including a second data packet and a second detection field; and

means for decoding the Received Encoded Packet to recover a copy of the sent data packet.

19. A system as described in claim 18, wherein the means for decoding comprises:

means for correcting errors in the Received Encoded Packet to recover a third Protected Packet, the third Protected Packet having a third data packet and a third detection field, the third Protected Packet including fields from the second Protected Packet with the errors being corrected, the third Protected Packet being a copy of the first Protected Packet within the power of the correction scheme.

20. A system as described in claim 19, wherein the means for decoding further comprises:

means for determining the integrity of the third Protected Packet; and

means for recovering a recovered data packet from the third Protected Packet, the recovered data packet being a copy of the sent data packet within the power of the correction and detection schemes.

21. A system as described in claim 19, wherein the means for correcting errors comprises means for correcting one or more errors occurred in a single data word of the Sent Encoded Packet only.

22. A system as described in claim 20, wherein the means for decoding comprises means for generating a packet drop indicator signal if the power of the correction scheme is exceeded and the correction scheme cannot correct errors.

23. A system as described claim 20, wherein the means for decoding comprises means for generating a packet drop indicator signal if the integrity of the third Protected Packet is not confirmed.

24. A system as described in claim 21, wherein the means for applying the error correction scheme to the first Protected Packet to add the first error correction field comprises means for applying an algebraic function to the data words in the first Protected Packet to generate the first error correction field.

25. A system as described in claim 19, wherein the means for correcting comprises:

means for applying an algebraic function to the data words in the second Protected Packet to generate a third error correction field;

means for applying bitwise exclusive OR function to the second and third correction fields to obtain an error syndrome value;

means for identifying the data word which has the error, if any, and means for obtaining a bit pattern of the error from the error syndrome value; and

means for correcting the identified word in the second Protected Packet by using the obtained bit pattern to obtain the third Protected Packet.

26. A system as described in claim 24, wherein the means for applying the algebraic function comprises means for performing a N-dimensional parity calculation.

27. A system as described in claim 26, wherein the means for performing the N-dimensional parity calculation comprises means for performing a 3D (three dimensional) parity calculation.

28. A system as described in claim 18, wherein the means for applying the error detection scheme comprises means for applying an algebraic function to the data words in the sent data packet to generate the first detection field.

29. A system as described in claim 28, wherein the means for applying the algebraic function comprises means for applying one or more of the following functions: CRC-16, CRC-32 and a checksum.

30. A system as described in claim 20, wherein the means for determining the integrity comprises:

means for applying said error detection scheme to the third data packet to generate a fourth detection field;

means for comparing the third and fourth detection fields; and

means for confirming the integrity of the third Protected Packet, if the third and fourth detection fields are equal.

31. A system as described in claim 27, wherein each data word is an 8-bit byte, and each data packet has not more than 64 bytes.

32. A system as described in claim 18, wherein the transmission medium comprises a transmission link.

33. A system as described in claim 32, wherein the transmission link comprises a line encoder for transforming each "p" bits of said sent encoded data packets into "q" bits, "q" being not less than "p", and a line decoder for transforming each of the received "q" bits into "p" bits of said received encoded data packets.

34. A system as described in claim 33, wherein "p"=8 and "q"=10.

35. An encoder for a transmission system for transmitting digital data in a form of packets through a transmission medium with error correction, comprising:

means for adding an error detection field to a sent data packet to form a Protected Packet;

means for adding an error correction field to the Protected Packet to form an encoded packet; and

means for sending the encoded packet to the transmission medium.

36. An encoder as described in claim 35, wherein the means for adding the error detection field comprises means for adding the error detection filed according to one the schemes: CRC-16, CRC-32 and checksum.

37. An encoder as described in claim 35, wherein the means for adding the error correction field comprises means for applying 3D parity calculation to the Protected Packet.

38. A decoder for a transmission system for transmitting digital data in a form of packets through a transmission medium with error correction, the decoder receiving comprising:

means for receiving a Received Encoded Packet from the transmission medium, the Received Encoded Packet being the encoded packet encoded by the encoder of claim 35 and transmitted through the transmission medium, the Received Encoded Packet including a Protected Packet and an error correction field;

means for correcting errors, if any, in the Received Encoded Packet to recover a corrected Protected Packet which includes fields from the Protected Packet with the errors being corrected;

means for determining integrity of the corrected Protected Packet; and

means for recovering a corrected data packet from the corrected Protected Packet, the corrected data packet being a copy of the sent data packet.